7 of 14 DOCUMENTS

THE WALL STREET JOURNAL.
The Wall Street Journal

October 8, 2005 Saturday

SECTION: Pg. B1

LENGTH: 1438 words

HEADLINE: **Identity Theft** -- Unplugged --- Despite the High-Tech Threat, When You Get Ripped Off It's Usually Still the Old Way

BYLINE: By **Robin Sidel**

BODY:

WORRIED THAT shadowy gangs of Russian hackers are breaking into computer networks, stealing your financial secrets? Don't lose too much sleep over it.

But you might want to hide your checkbook when friends and relatives come visit your home.

Despite a series of alarming reports in recent months about security breaches that have made personal data potentially vulnerable to crooks -- such as the one at credit-card processor CardSystems Solutions Inc. affecting 40 million credit-card accounts -- most bank-related crimes remain stubbornly low-tech. They range from simple forgery of a check, to unauthorized credit-card use, to Dumpster-diving, which is when someone plucks a bank statement or credit-card bill from your garbage.

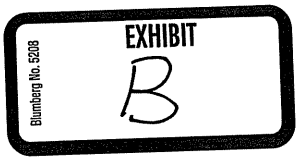
And the perpetrator probably may not be a stranger.

According to one recent study, by Javelin Strategy & Research, a consulting firm in Pleasanton, Calif., in 26% of all cases the fraud victims knew the person who had misused their personal information. (Typically it was a family member, friend or neighbor, or in-home employee.) In addition, as much as 50% of debit-card fraud occurs when a card is snagged by a family member or friend who knows the card's personal-identification number, according to a recent report from TowerGroup, a unit of MasterCard International Inc.

The term "**identity theft**" is often used loosely to describe a wide array of crimes. But true **identity theft** occurs when someone uses stolen information to create a new form of identity, such as opening a new credit-card account under the victim's name. That differs significantly from other kinds of bank fraud, such as when a criminal uses a stolen ATM card to get cash out of a teller machine.

Whether it's full-blown ID theft or small-scale fraud, even in cases where the criminal is a stranger, it's almost never a case of sophisticated computer hacking. Although 75% of all households use the Internet and 65% of those do some online banking, "most criminals obtain personal information through traditional rather than electronic channels," according to the Javelin study. Some 29% of victims surveyed said their personal information was obtained through a lost or stolen wallet, checkbook or credit card.

According to the study, the bulk of the rest were attributed to friends and relatives, corrupt employees, stolen mail, Dumpster-diving, and computer spyware. Computer viruses or hackers accounted for only 2.2% of incidents. While



there has been a significant increase in the number of electronic attempts at **identity theft,** "the ones that are working are the traditional ones," said James Van Dyke, Javelin's president.

The Federal Trade Commission itself defines **identity theft** broadly, describing it as when someone possesses or uses a person's personal or financial information without their knowledge with the intent of committing fraud or other crimes.

The commission estimates that **identity theft** affects nearly 5% of the adult population, costing businesses and individuals a combined $53 billion annually. It received 246,000 reports of **identity theft** last year, nearly triple the number received in 2001. The FTC has attributed much of that rise to heightened awareness of the issue among consumers, making them more likely to report incidents as **identity theft.**

Overall, statistics on **identity theft** are spotty. For one thing, research has found that most victims of **identity theft** don't report the crime to police. In many cases, they aren't even certain that they are truly crime victims and don't know how the incident occurred. Banks increasingly alert authorities when incidents occur, but even those disclosures can be incomplete.

There are a number of steps individuals can take to protect themselves.

Many financial institutions are increasingly urging their clients to start using paper shredders at home. Household models can be relatively inexpensive, and they significantly reduce the chances that a criminal can find any useful personal information in the trash. Banks typically recommend shredding documents that contain account information, Social Security numbers, credit-card and ATM receipts and credit-card offers. Also, shred blank checks that sometimes come in the mail as part of a solicitation.

Another suggestion: Be particularly aware if credit-card bills or bank statements are missing from the mailbox. If a bill arrives more than two weeks late, the American Bankers Association suggests contacting the local post office to be sure it isn't being forwarded without the recipient's knowledge. Also check with the company where the bill originated.

It's also wise to avoid disclosing any personal information on forms or applications unless absolutely necessary, says Mike Cunningham, senior vice president in the credit-card fraud department at J.P. Morgan Chase & Co.

As an example, Mr. Cunningham says, he was recently filling out an application to be a coach on his son's neighborhood football team in Arizona, and the form asked for his social security number, driver's license number and other personal information. He declined to provide the information, because there was no way for him to know whether his personal information would be kept under lock and key.

"I just told the team mom that I didn't see why they needed it -- it was the perfect amount of information for an identity thief," he said. He got the job anyway.

The only organizations you're required to provide with your social security number are your employer and your financial institutions. (This is for tax purposes.) If anyone else asks -- say, a retailer -- you don't have to give it. The company can decline to provide the service, but it's worth asking what other identification they might accept instead.

Amid the proliferation of old-fashioned fraud, some financial institutions are fighting back by urging their customers to abandon paper statements altogether and instead view their accounts online. Among them is E*Trade Financial Corp., which says its online system is more secure than paper statements that can be stolen or copied. A spokeswoman declined to specify how much money the company will save by eliminating the printing and mailing of paper statements.

Banks are having a particularly tough time battling one of the oldest and most common kinds of crime: check fraud. Attempts of check fraud rose to $5.5 billion in 2003 from $4.3 billion in 2001, according to the American Bankers Association. The incidents resulted in losses of $677 million, representing a slight decline from $698 million in 2001; the trade group attributed the drop to better fraud-detection methods.

That slight decline isn't so reassuring to Lee Roberts, senior vice president at National Penn Bancshares Inc., a regional bank based in Boyertown, Pa. As recently as the past few weeks, the bank has been hit by a wave of incidents in which criminals have copied checks and then altered them for fraudulent use. That practice "has been around for seven or eight years," says Mr. Roberts. But as photocopiers and image-manipulation computer software become more sophisticated, he says, "they're getting better at it."

Identity Theft -- Unplugged --- Despite the High-Tech Threat, When You Get Ripped Off It's Usually Still the Old Way
The Wall Street Journal October 8, 2005 Saturday

Battling **Identity Theft**

Despite all the buzz about high-tech online **identity theft**, most instances revolve around old-fashioned fraud such as forging a signature on a check. Here are steps for reducing the risk:

-- Check up on yourself regularly
Get a copy of your credit report every year from each of the major credit bureaus (TransUnion, Equifax, Experian) to make sure the records are accurate. Also, closely review all monthly bank and billing statements for discrepancies.

-- Travel light
Avoid carrying around credit-card or personal documents unless you really need them.

-- Keep personal data under wraps
Don't share personal ID numbers or passwords with anyone. Don't provide information over the phone or hand over personal data unless you know why it is needed. Keep a list of all account numbers in a secure place so that you have quick access if cards or documents get stolen or lost.

-- Buy a shredder for the home
Tear up or shred all credit-card receipts and all new-card offers that arrive in mail. Also destroy all documents that contain account numbers or other personal financial information.

-- Check the mail
Don't let mail sit in the mailbox for days on end. And don't place sensitive outgoing mail, such as bills, in your home mailbox to await collection. Instead, drop it in a collection box.

Sources: Federal Trade Commission, American Bankers Association

NOTES:
PUBLISHER: Dow Jones & Company, Inc.

LOAD-DATE: October 8, 2005